What is claimed is:

CLAIMS

1. A digital signature cryptographic method comprising:

supplying a set S1 of k polynomial functions as a public-key, the set S1 including the functions $P_1(x_1,...,x_{n+v}, y_1,...,y_k),..., P_k(x_1,...,x_{n+v}, y_1,...,y_k)$, where k, v, and n are integers, $x_1,...,x_{n+v}$ are n+v variables of a first type, $y_1,...,y_k$ are k variables of a second type, and the set S1 is obtained by applying a secret key operation on a set S2 of k polynomial functions $P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$ where $a_1,...,a_{n+v}$ are n+v variables which include a set of n "oil" variables $a_1,...,a_n$, and a set of v "vinegar" variables $a_{n+1},...,a_{n+v}$;

providing a message to be signed;

applying a hash function on the message to produce a series of k values $b_1,...,b_k$;

substituting the series of k values $b_1,...,b_k$ for the variables $y_1,...,y_k$ of the set S2 respectively to produce a set S3 of k polynomial functions $P''_1(a_1,...,a_{n+v}),..., P''_k(a_1,...,a_{n+v})$;

selecting v values $a'_{n+1},...,a'_{n+v}$ for the v "vinegar" variables $a_{n+1},...,a_{n+v}$;

solving a set of equations $P''_1(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0,..., P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$ to obtain a solution for $a'_1,...,a'_n$; and

applying the secret key operation to transform $a'_1,...,a'_{n+v}$ to a digital signature $e_1,...,e_{n+v}$.

2. A method according to claim 1 and also comprising the step of verifying the digital signature.

3. A method according to claim 2 and wherein said verifying step comprises the steps of:

obtaining the signature $e_1,...,e_{n+v}$, the message, the hash function and the public key;

applying the hash function on the message to produce the series of k values $b_1,...,b_k$; and

verifying that the equations $P_1(e_1,...,e_{n+v},b_1,...,b_k)=0,...,$ $P_k(e_1,...,e_{n+v}, b_1,...,b_k)=0$ are satisfied.

4. A method according to claim 1 and wherein the set S2 comprises the set f(a) of k polynomial functions of the HFEV scheme.

5. A method according to claim 1 and wherein the set S2 comprises the set S of k polynomial functions of the UOV scheme.

6. A method according to claim 1 and wherein said supplying step comprises the step of selecting the number v of "vinegar" variables to be greater than the number n of "oil" variables.

7. A method according to claim 1 and wherein v is selected such that q^v is greater than 2^{32}, where q is the number of elements of a finite field K.

8. A method according to claim 1 and wherein said supplying step comprises the step of obtaining the set S1 from a subset S2' of k polynomial functions of the set S2, the subset S2' being characterized by that all coefficients of components involving any of the $y_1,...,y_k$ variables in the k polynomial functions $P'_1(a_1,...,a_{n+v},y_1,...y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$ are zero, and the number v of "vinegar" variables is greater than the number n of "oil" variables.

9. A method according to claim 8 and wherein the set S2 comprises the set S of k polynomial functions of the UOV scheme, and the number v of "vinegar" variables is selected so as to satisfy one of the following conditions:

(a) for each characteristic p other than 2 of a field K in an "Oil and Vinegar" scheme of degree 2, v satisfies the inequality $q^{(v-n)-1} * n^4 > 2^{40}$,

(b) for p = 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n*(1 + sqrt(3)) and lower than or equal to $n^3/6$, and

(c) for each p other than 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n and lower than or equal to n^4.

10. A method according to claim 8 and wherein the set S2 comprises the set S of k polynomial functions of the UOV scheme, and the number v of "vinegar" variables is selected so as to satisfy the inequalities $v<n^2$ and $q^{(v-n)-1} * n^4 > 2^{40}$ for a characteristic p=2 of a field K in an "Oil and Vinegar" scheme of degree 2.

11. A method according to claim 1 and wherein said secret key operation comprises a secret affine transformation s on the n+v variables $a_1,\ldots,a_{n+v}$.

12. A method according to claim 4 and wherein said set S2 comprises an expression including k functions that are derived from a univariate polynomial.

13. A method according to claim 12 and wherein said univariate polynomial includes a univariate polynomial of degree less than or equal to 100,000.

14. A cryptographic method for verifying the digital signature of claim 1, the method comprising:

obtaining the signature $e_1,...,e_{n+v}$, the message, the hash function and the public key;

applying the hash function on the message to produce the series of k values $b_1,\ldots,b_k$; and

verifying that the equations $P_1(e_1,...,e_{n+v},b_1,\ldots,b_k)=0,\ldots,$ $P_k(e_1,...,e_{n+v}, b_1,\ldots,b_k)=0$ are satisfied.

15. In an "Oil and Vinegar" signature method, an improvement comprising the step of using more "vinegar" variables than "oil" variables.

16. A method according to claim 15 and wherein the number v of "vinegar" variables is selected so as to satisfy one of the following conditions:

(a) for each characteristic p other than 2 of a field K and for a degree 2 of the "Oil and Vinegar" signature method, v satisfies the inequality $q^{(v-n)-1} * n^4 > 2^{40}$,

(b) for p = 2 and for a degree 3 of the "Oil and Vinegar" signature method, v is greater than n*(1 + sqrt(3)) and lower than or equal to $n^3/6$, and

(c) for each p other than 2 and for a degree 3 of the "Oil and Vinegar" signature method, v is greater than n and lower than or equal to n^4.

17. A method according to claim 15 and wherein the set S2 comprises the set S of k polynomial functions of the UOV scheme, and the number v of "vinegar" variables is selected so as to satisfy the inequalities $v<n^2$ and $q^{(v-n)-1} * n^4 > 2^{40}$ for a characteristic p=2 of a field K in an "Oil and Vinegar" scheme of degree 2.

Add A3

Add B3